Snode

The Noise Before Defeat

The Need For Holistic And Strategic Threat Management Programs

Snode

"**Strategy** without tactics is the slowest route to victory. **Tactics** without strategy is the noise before defeat".

Snode

This is what the noise before defec
looks like.

Snode

The Epistemology of Strategy

Strategy, in warfare, is the science or art of employing all the military, economic, political, and other resources of a country to achieve the objects of war.

Snode

Why Strategy?

Because Risk.

Probability x Impact = Risk

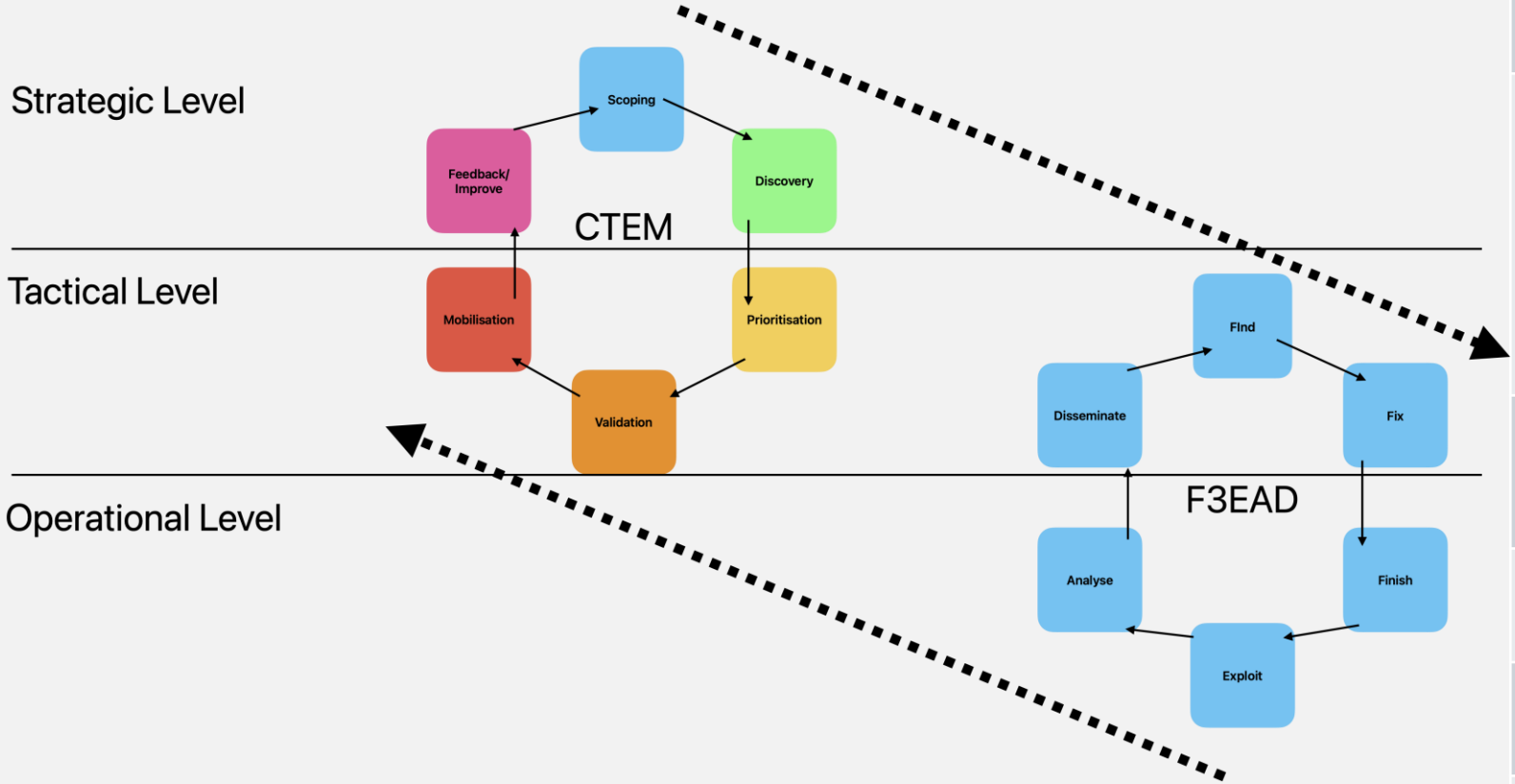
Snode

$\frac{\text{Silhouette}}{\text{Deception}} \times \frac{\text{Vulnerability}^{\text{Asset}}}{\text{Controls}} = \text{Exposure}$

Adversaries see an organisation’s cyber silhouette → Vulnerabilities are targeted to gain access to assets → Assets are categorised by criticality → Deception conceals or disrupts the silhouette → Control covers the exposure surface → less exposure = less risk

Snode

From The Strategic To The Operational



F3EAD	Description
Find	Essentially 'picking up the scent' of the adversary, with the classic "Who, What, When, Where, and Why" questions being used within this phase to identify a candidate target.
Fix	Verification of the target(s) identified within the previous phase, which typically involves multiple data points. This phase effectively transforms the intelligence gained within the "Find" phase into evidence that can be used as basis for action within the next stage.
Finish	Based on the evidence generated from the previous two phases, the commander of the operation then imposes their will on the target.
Exploit	Deconstruction of the evidence generated from the finish phase.
Analyse	Results are analysed to answer the intelligence requirements.
Disseminate	Integrate exploited intel with the wider intelligence picture.

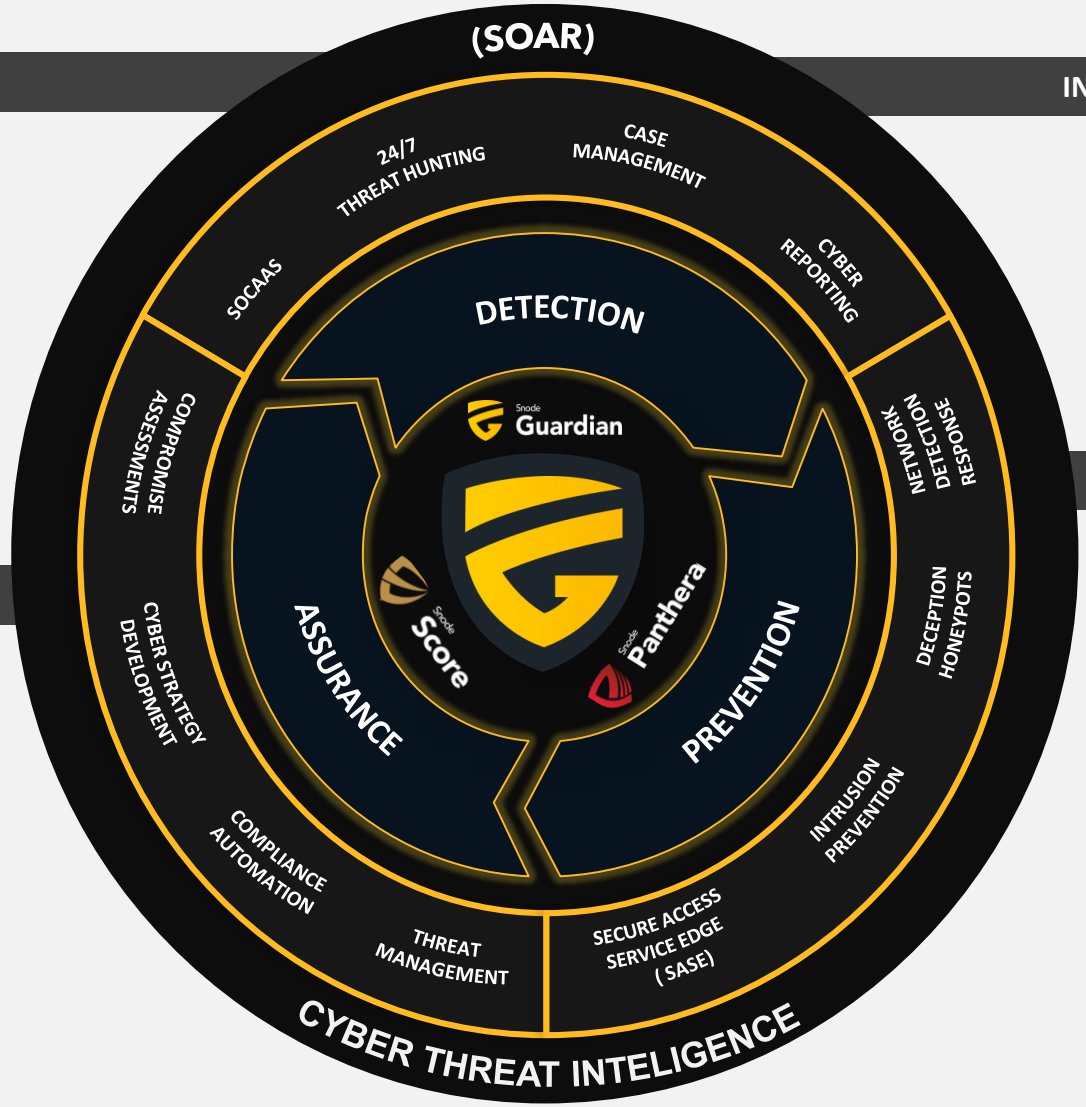
Threat Management Program

GUARDIAN

- Environment readiness assessment
- Secure node placement
- End-to-end coverage
- Threat hunting & first responder training
- Threat lifecycle controls
- Ingestion opportunities
- Deception technology
- Automated defence & risk reduction
- Custom detection use cases

ASSURANCE & MANAGEMENT REPORTING

- Incident workflows maturity
- Incident response metrics
- Framework visualisation
- Incident response performance
- Policy violation monitoring
- Native asset management
- VMI – fusion of risk sources



INCIDENT RESPONSE PROGRAM

- Tabletop exercise
- IRP development
- Defence-in-depth repository
- Risk-based exception handling/reporting
- Playbook & battle box development
- CSIRT assist response retainers
- Rehearsals, informed/uninformed

SPECIALISED RISK REDUCTION SERVICES

- Vulnerability management practice implementation
- Cyber risk treatment policy development
- Capability maturity assessments
- Cyber strategy development
- Attack surface visualization
- Deceptive tech strategy development
- VAPT & webapp assessments
- Dark web analysis & threat modeling.
- Inline and independent forensic investigations

Snode

How To Articulate Risk

1 Align Cyber Risk with Organisational Objectives

- Speak the Language of Business
- Quantify the Risk

2 Prioritise Risks Based on Impact

- Focus on High-Impact Threats
- Use Risk Scenarios

3 Emphasize ROI and Competitive Advantage

- Cost-benefit Analysis
- Competitive Edge

4 Simplify Communication

- Avoid Jargon
- Use Visuals

5 Propose Clear, Actionable Plans

- Present Solutions, Not Just Problems
- Demonstrate Preparedness

6 Highlight Regulatory and Legal Implications

- Compliance Focus
- Legal Risks

Snode

Thank You, Let’s Connect